Shubham Paikrao

🎯 Insider Threat

🚨 1. Identification

Detection Methods	- DLP alerts - SIEM anomalies - Endpoint monitoring - User reports - Access outside work hours or unusual geolocation - Mass downloads or transfers
Red Flags	- Accessing files unrelated to the job - Forwarding sensitive files to a personal email - Deleting logs or disabling controls - Disgruntled behavior or recent HR action
Initial Triage	- Identify user(s) involved - Scope of unauthorized access - Determine if the real-time threat is ongoing

---

🧯 2. Containment

Immediate Containment	- Disable user accounts (AD, VPN, SaaS) - Block network access - Prevent remote logins and email forwarding
Preserve Evidence	- Do not wipe the device yet - Image affected systems and copy logs - Monitor user activity in stealth if the ongoing investigation is needed
Secure Data Assets	- Restrict access to affected files - Apply audit logs and retention for involved repositories
Coordinate with HR & Legal	- If the user is active, involve HR for controlled confrontation - Legal must review investigation boundaries

3. 🔬 Investigation

Forensic Imaging	Create disk and memory images of endpoint(s). Do not alter original evidence.
Log Review	Analyze: - File access logs - VPN/remote access logs - Email forwarding rules - USB connection logs - GitHub/Cloud uploads
Data Access Audit	Identify what sensitive/confidential data was accessed, copied, or moved.
Behavioral Timeline	Build a timeline of suspicious activities: first sign to containment.
Stakeholder Interviews	Interview supervisors, coworkers, and HR for context and behavioral patterns.
Legal & Compliance Review	Ensure all investigative steps are legally defensible (e.g., wiretapping laws, employee rights).

---

4. 🛠 Remediation & 🩺 Recovery

System Cleanup	- Remove backdoors, exfil scripts, and scheduled tasks - Close accounts and reset access controls
Restore File Integrity	- Check for altered or deleted data and restore from backup if needed
Patch Access Gaps	- Implement least privilege where abuse occurred - Remove orphaned or unnecessary accounts
HR Disciplinary Action	- Depending on findings: reprimand, suspension, termination, or legal referral
Update Monitoring Rules	- Add new behavior indicators to detection systems for future alerts

---

📝 5. Reporting & Documentation

📁 5.1 Evidence Collected

- Endpoint forensic images
- Email logs and attachments
- Security camera footage (if applicable)
- DLP alerts and file transfer logs
- Employee chat history (Teams, Slack)
- Witness statements/interviews

📜 5.2 Timeline of Events

- Time
- Action taken

📬 5.3 Communications & Notification

- Audience
- Method
- Notes

🔁 6. Lessons Learned / Review

What worked well? (e.g., fast detection, good containment)

What failed? (e.g., over-privileged access, lack of logging)

Preventative actions:

- Tighten access reviews
- Increase user behavior monitoring
- Expand DLP rules
- Adjust the offboarding process

✅ Quick Checklist

- ✅ Detect unusual activity
- ✅ Isolate user access
- ✅ Preserve evidence
- ✅ Forensic analysis
- ✅ Notify HR/Legal
- ✅ Interview and document
- ✅ Patch process gaps
- ✅ Conduct lessons learned